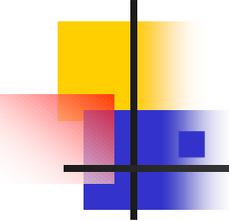


# FIPS 140-2 and the Cryptographic Module Validation Program (CMVP)

---

Annabelle Lee  
Director, CMVP  
March 26, 2002

# FIPS 140-2 and CMVP

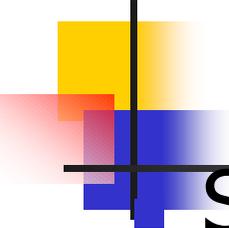


## ■ CMVP is a dynamic program

---

- Learning process for validation authorities
- FIPS 140-1 & 2 and DTR constantly reexamined
  - Implementation Guidance
  - Technical and Program Policy
  - Technical questions submitted by laboratories
    - Specific issue or general topic
    - Standardized form and content
- Validation Reports reevaluated for enhancement
- Questions from vendor and user communities provide valuable input

# FIPS 140-2: Summary of Changes



- Standard has not changed in **focus** or **emphasis**
- Language and terminology
  - **Standardized** and **updated** to add clarity and consistency
- Redundant and extraneous information removed
  - New standard is more **concise**
- Vague requirements removed or revised
- Standard was minimally restructured

# FIPS 140-1 & 2 Tables of Contents

## FIPS 140-1

1. Overview
2. Glossary of Terms and Acronyms
3. Functional Security Requirements
4. Security Requirements
  - 4.1 Cryptographic Modules
  - 4.2 Cryptographic Module Interfaces

## FIPS 140-2

1. Overview
2. Glossary of Terms and Acronyms\*
3. Functional Security Requirements
4. Security Requirements
  - 4.1 Cryptographic Module Specification\*
  - 4.2 Cryptographic Module Ports and Interfaces

\* Section added or revised

# FIPS 140-1 & 2 Tables of Contents

(Continued)

## FIPS 140-1

- 4.3 Roles and Services
- 4.4 Finite State Machine Model
- 4.5 Physical Security
- 4.6 Software Security
- 4.7 Operating System Security
- 4.8 Cryptographic Key Management

## FIPS 140-2

- 4.3 Roles, Services, and Authentication
- 4.4 Finite State Model
- 4.5 Physical Security\*
- 4.6 Operational Environment\*
- 4.7 Cryptographic Key Management

\* Section added or revised

# FIPS 140-1 & 2 Tables of Contents

(Continued)

## FIPS 140-1

- 4.9 Cryptographic Algorithms
- 4.10 EMI/EMC
- 4.11 Self-Tests

## FIPS 140-2

- 4.8 EMI/EMC
- 4.9 Self-Tests
- 4.10 Design Assurance\*
- 4.11 Mitigation of Other Attacks\*

\* Section added or revised

# FIPS 140-1 & 2 Tables of Contents

(Concluded)

## FIPS 140-1

### Appendices

A: Summary of Documentation Requirements

B: Recommended Software Development Practices

C: Selected References

## FIPS 140-2

### Appendices

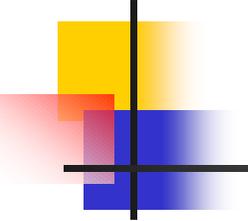
A: Summary of Documentation Requirements

**B: Recommended Software Development Practices\***

**C: Cryptographic Module Security Policy\***

**D: Selected Bibliography\***

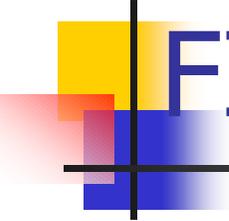
\* Section added or revised



# Summary of Changes from FIPS 140-1 to FIPS 140-2

---

- Cryptographic Module Specification
  - *Primary modification:* inclusion of the approved algorithms and security functions
- Cryptographic Module Ports and Interfaces
  - *Primary modification:* physically separate ports *and* logical separation within existing physical ports via a trusted path
    - Applicable to plaintext I/O



# Summary of Changes from FIPS 140-1 to FIPS 140-2 (cont.)

---

- Roles, Services, and Authentication
  - *Primary modification:* Addition of strength of mechanism requirements for authentication
- Finite State Model
  - *Primary modification:* Reference to a Finite State Model to better represent both hardware, firmware, and software modules

# Summary of Changes from FIPS 140-1 to FIPS 140-2 (cont.)

---

- Physical Security
  - *Primary modification:* Reorganization of the subsections for consistency and clarity
- Operational Environment
  - *Primary modification:* Replacement of the TCSEC requirements with CC requirements
- Cryptographic Key Management
  - *Primary modifications:* Addition of Over-The-Air-Rekeying (OTAR) for radios, addition of strength of mechanism requirements for Key Establishment

# Summary of Changes from FIPS 140-1 to FIPS 140-2 (cont.)

## Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

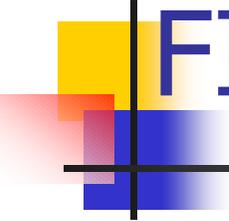
- *Primary modification:* Modified to reflect changes in FCC requirements

## ■ Self-Tests

- *Primary modification:* Strengthened the required statistical Random Number Generator (RNG) tests and better addressed bypass mode

## ■ Design Assurance

- *Primary modification:* Formerly the Design Assurance Section, expanded to include: configuration management, correct delivery, and guidance documentation



# Summary of Changes from FIPS 140-1 to FIPS 140-2 (cont.)

---

- Mitigation of Other Attacks
  - *New Section*: Provides information, recommendations, and requirements for new types of cryptographic attacks
- Appendixes
  - *A. Summary of Documentation Requirements*: updated
  - *B. Recommended Software Development Practices*: updated



# Summary of Changes from FIPS 140-1 to FIPS 140-2 (cont.)

---

- Appendixes (concluded)
  - *C. Security Policy*: Mandates requirements for the content and structure of the security policy
  - *D. Selected Bibliography*: updated

# Summary of Changes from FIPS 140-1 to FIPS 140-2 (concluded.)

---

- Annex A: *Approved Security Functions*
- Annex B: *Approved Protection Profiles*
- Annex C: *Approved Random Number*
- Annex D: *Approved Key Establishment Techniques*